

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-312321

(43) 公開日 平成10年(1998)11月24日

(51) Int.Cl.⁹

G 0 6 F 11/32
13/00
15/00

識別記号

3 5 1
3 2 0

F I

G 0 6 F 11/32
13/00
15/00

E

3 5 1 N
3 2 0 K

審査請求 未請求 請求項の数 3 O L (全 9 頁)

(21) 出願番号

特願平9-120484

(22) 出願日

平成9年(1997)5月12日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 小暮 慎一

東京都江東区新砂一丁目6番27号 株式会

社日立製作所公共情報事業部内

(74) 代理人 弁理士 小川 勝男

(54) 【発明の名称】 オンラインシステム障害解析方法

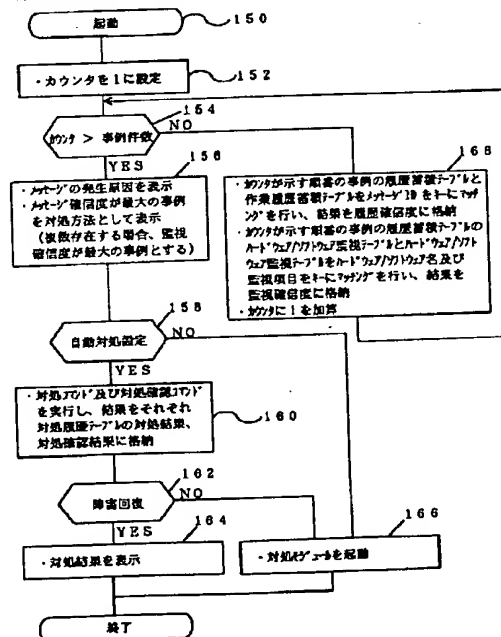
(57) 【要約】

【課題】 本発明はオンラインシステムの障害の検出から対処方法の表示までの処理をリアルタイムに実現し、障害による影響を最小限に抑えることにある。

【解決手段】 障害メッセージ発生時、カウンタを1にする(ステップ152)。メッセージテーブルの全事例についてカウンタの示す順番の事例の履歴確信度及び監視確信度を求める(ステップ168)。障害メッセージの発生原因の表示を行い、メッセージテーブルに格納されている履歴確信度が最大の事例を最適対処方法として表示する(履歴確信度が最大の履歴が複数存在する場合には監視確信度が最大の事例を表示する)(ステップ156)。対処が自動的に設定されている場合、対処コマンド及び対処確認コマンドを実行し(ステップ160)。障害が回復した場合は対処結果を表示し(ステップ164)、回復しない場合は対処モジュールを起動し人による対処を行う(ステップ166)。

図3

<障害解析モジュール>



【特許請求の範囲】

【請求項1】 システムから出力されるデータに係る情報を蓄積し、障害に関する情報と、システムから出力されるデータに係る情報との対応関係を検査し、対応が一致したときは、障害に係る原因と、障害の対処方法の表示を実現することを特徴とする障害解析方法。

【請求項2】 請求項1において、ハードウェアの監視と、ソフトウェアの監視を常時行い、ハードウェア及びソフトウェアの障害について、障害に関する原因と、障害の対処方法の表示を実現することを特徴とする障害解析方法。

【請求項3】 請求項2において、障害に関する情報は、障害の原因に係る情報と、過去の障害の事例に係る情報を管理することを特徴とする障害解析方法。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明はシステムから出力される情報からハードウェア及びソフトウェアの障害について、障害に関する原因と、障害の対処方法の表示を実現する障害解析方法に関し、特に障害の検出から対処までの処理に高速なリアルタイム性を要求されるオンラインシステムに関する。

【0002】

【従来の技術】 機器などのハードウェアの障害やアプリケーションプログラムなどのソフトウェアの障害に関し、障害の診断を行う装置やシステムが様々な分野で開発され、稼動している。これらのシステムの管理においては、障害解析が大きな役割を果たしている。例えば、特開平06-161760号公報に示されているように機器の診断にリアルタイム性を持った装置を持ったものがある。この技術では、専門家によって行われていた診断を機械化することによって判定にばらつきがなく、迅速な診断を可能としている。また、特開平08-237188号公報に示されているように通信端末装置は通信の履歴に関するデータを記憶し、通信障害時のデータをネットワークを介して情報蓄積装置に伝送することにより、通信端末装置の保守を効率良くできるようにしている。

【0003】 また、企業や官庁において、高速処理や信頼性が要求される分野で様々なオンラインシステムが稼動している。これらのシステムにおいては、機器などのハードウェア上でアプリケーションプログラムなどのソフトウェアが稼動しており、個々のハードウェアやソフトウェアの障害の診断を行っている。

【0004】

【発明が解決しようとする課題】 かかる従来の方法においては、次のような問題がある。

【0005】 すなわち、ハードウェアとソフトウェアの

障害が同時に複数件発生した場合、障害の検出から障害の対処までの処理を高速に実現することは困難な作業となる。

【0006】 このように従来の方法は、ハードウェアまたはソフトウェアの個々の障害に対応するもので、複数のハードウェア装置及びソフトウェアから構成され相互に影響を与える可能性のあるシステムの障害には対処できないという問題があった。

【0007】 本発明の目的は、複数のハードウェア装置及びソフトウェアから構成されるオンラインシステムの障害にリアルタイムに対処可能なオンラインシステム障害解析方法を提供することにある。

【0008】 本発明の他の目的は、従来人間が行っていた複雑な障害回復作業を機械化することにより作業の精度及び速度の向上や作業の容易性を実現し、障害による損害を最小限に抑えて、専門の知識を持たない人でも障害回復作業を行うための手段を提供することにある。

【0009】

【課題を解決するための手段】 本発明は、オンラインシステムから監視端末に出力されるメッセージの履歴に係る情報の一定期間の蓄積とハードウェア/ソフトウェアの稼動状況の監視を行い、障害が発生した際に、障害の原因の表示と過去の最適事例の対処方法の表示を行う。

【0010】 オンラインシステムから監視端末に出力されるメッセージをメッセージ監視モジュールにおいて常時監視し、出力メッセージの一定時間の履歴を随時、履歴蓄積テーブルに蓄積しておく。障害が発生した際には、障害発生時点の履歴蓄積テーブルを作業履歴蓄積テーブルとしてコピーする。この作業履歴蓄積テーブルとメッセージテーブルの過去の事例の履歴をメッセージIDをキーにマッチングを行い、一致した数を履歴確信度として格納する。続いて、障害が発生した時点のハードウェア/ソフトウェアの稼動状況とメッセージテーブルの過去の事例が発生した時点のハードウェア/ソフトウェアの稼動状況をハードウェア/ソフトウェア名及び監視項目をキーにマッチングを行い、一致した数を監視確信度として格納する。そして、履歴確信度が最大の事例を最適事例とする（履歴確信度が最大の事例が複数存在する際には、監視確信度が最大の事例とする）。なお、障害メッセージの原因及び分類情報、過去の事例情報はメッセージテーブルで管理する。続いて、障害の原因の表示と最適事例の対処方法の表示を行う。対処による障害回復については、対処コマンドと対処確認コマンドの実行及び結果確認により行う。

【0011】 ハードウェアの監視と、ソフトウェアの監視を常時行い、ハードウェア及びソフトウェアの障害について、障害に関する原因と、障害の対処方法の表示をリアルタイムに実現することを特徴とする障害解析方法。

【0012】障害に関係する情報は、障害の原因に関する情報と、過去の障害の事例に関する情報の2種類とする。

【0013】

【発明の実施の形態】以下、本発明の実施の形態を詳細に説明する。

【0014】図1、図2、図3、図4は、本発明をオンラインシステムに適用した場合の処理手順の実施の形態を示すフローチャートであり、図5は、本発明に係るオンラインシステム障害解析方法の構成を示すブロック図である。図6及び図7は、本発明に係るオンラインシステム障害解析方法を実現する際に利用するデータテーブルである。

【0015】図5において、障害解析処理を監視端末における5つのモジュールにより実現する。メッセージ監視モジュール12は、まず、オンラインシステム10からメッセージ取得部11を通じて監視端末側へ出力される全てのメッセージを履歴蓄積テーブル17へ格納する。次に、出力メッセージに関する分類情報をメッセージテーブル19へ参照し、履歴蓄積テーブル17へ格納する。ハードウェア監視モジュール13は、ハードウェア稼動状況を常時監視しており、ハードウェア監視テーブル20に格納する。ソフトウェア監視モジュール14は、ソフトウェア稼動状況を常時監視しており、ソフトウェア監視テーブル21に格納する。履歴蓄積テーブル17は、オンラインシステム10から出力されるメッセージの履歴に関する情報を蓄積する為に用いられる。作業履歴蓄積テーブル18は、障害発生時点のメッセージの履歴に確保し、メッセージテーブルの過去の事例の履歴との比較を行う為に用いられる。対処履歴テーブル22は、障害発生後の対処結果を格納する為に用いられる。メッセージテーブル19には、監視対象のメッセージがメッセージIDをキーとして、ハードウェア/ソフトウェア別、システムメッセージ/アプリケーションメッセージ別に分類した形で格納されている。ハードウェア監視テーブル20は、ハードウェアの稼動状況を常時監視する為のテーブルであり、監視対象の設定は予め設定しておくものとする。ソフトウェア監視テーブル21は、ソフトウェアの稼動状況を常時監視する為のテーブルであり、監視対象の設定は予め設定しておくものとする。障害解析モジュール15は、障害が発生した際に起動され、障害の原因の表示と過去の最適事例の対処方法の表示を行い、対処結果を対処履歴テーブル22に格納する。対処履歴テーブル22は、発生した障害メッセージに対する対処の情報を格納する為のテーブルである。

【0016】図6及び図7は、図5における各テーブルのレコードフォーマットであり、以下、図6及び図7の各テーブルの関係について説明する。図6A<履歴蓄積テーブル及び作業履歴蓄積テーブル>は、図5の履歴蓄積テーブル17及び作業履歴蓄積テーブル18のレコー

ドフォーマットである。ここで、図6A<履歴蓄積テーブル及び作業履歴蓄積テーブル>の各項目について説明する。メッセージIDは図5のオンラインシステム10から図5の監視端末に出力されるメッセージを識別するキーとして用い、メッセージが発生する度に図5A<履歴蓄積テーブル>に蓄積される。発生時刻にはメッセージが出力された時刻を格納する。ソフト/ハード区分及び障害/警告区分には図6B<メッセージテーブル>を参照し、格納する。メッセージには出力されたメッセージの中のコメント情報をテキスト形式で格納する。図6B<メッセージテーブル>は、図5のメッセージテーブル19のレコードフォーマットである。続いて、図6B<メッセージテーブル>の各項目について説明する。メッセージIDは図6B<メッセージテーブル>におけるキーとして管理されており、ハードウェア/ソフトウェア別、システムメッセージ/アプリケーションメッセージ別に分類されている。障害/警告区分はメッセージが障害を意味するか警告を意味するかを示すものである。原因はマニュアルに掲載されている情報であり、重要度はメッセージの持つ意味合いを示すものである。事例件数は、過去の事例を図6B<メッセージテーブル>に何件格納してあるかを示す。障害メッセージについてのみ、過去の事例が発生した時の出力メッセージの履歴を履歴蓄積テーブルで、過去の事例の対処に関する情報を対処テーブルでそれぞれ管理している。続いて、図6C<対処テーブル>の各項目について説明する。図6C<対処テーブル>には発生した障害に対して行った対処方法を格納する。対処策には実際の対処策の内容を格納する。対処コマンドには実際の対処に用いたコマンドを格納し、対処結果コマンドには対処コマンドの実行結果を格納する。対処確認コマンドには対処コマンドが正しく実行されたかを確認するコマンドを格納し、対処確認結果には対処確認コマンドの実行結果の確認事項を格納する。履歴確信度には障害発生時点の図6A<作業履歴蓄積テーブル>と図6B<メッセージテーブル>に格納されている事例の履歴蓄積テーブルとのメッセージIDをキーとしたマッチングの結果を格納する。監視確信度には障害発生時点のハードウェア/ソフトウェア稼動状況をハードウェア/ソフトウェア名及び監視項目をキーとしたマッチングの結果を格納する。自動/手動対処設定には、過去の障害の中で最も確信度が高かった場合に自動的に対処を行うかどうかを設定する。続いて、図7D<ハードウェア監視テーブル>は、図5のハードウェア監視テーブル20のレコードフォーマットであり、ハードウェア別に監視項目及び監視結果を設定する。図7E<ソフトウェア監視テーブル>は、図5のソフトウェア監視テーブル21のレコードフォーマットであり、ソフトウェア別に監視項目及び監視結果を設定する。図7F<対処履歴テーブル>は、図5の対処履歴テーブル22のレコードフォーマットであり、発生した障害メッセー

ジに対する対処が終了した時点で格納する為のテーブルであり、障害解析が終了した時点で図4のメッセージテーブル19に事例として格納する。

【0017】次に図1、図2、図3、図4のフローチャートに基いて図5の各動作を説明する。

【0018】図5のメッセージ監視モジュール12の起動(ステップ100)から終了までの動作を説明する。障害解析を終了するまで処理を行う(ステップ102)。まず、図5のオンラインシステム10よりメッセージが出力されているかを確認する(ステップ104)。出力されていればメッセージIDをキーに図5のメッセージテーブル19を参照し、図5の履歴蓄積テーブル17に出力メッセージに関する情報を蓄積する(ステップ106)。蓄積する際、図5メッセージテーブル19からメッセージID、発生時刻、ソフト/ハード区分、障害/警告区分、メッセージを参照する。図5のメッセージテーブル19に登録されていないメッセージが出力された場合には履歴蓄積テーブルへの蓄積を行わない。次に、出力メッセージが障害メッセージであるかを判別し(ステップ108)、障害である場合以下の処理を行う。まず、障害メッセージ発生時点の履歴蓄積テーブルを作業履歴蓄積テーブルとしてコピーする(ステップ110)。続いて、障害メッセージがハードウェアに関するものであれば(ステップ112)、ハードウェア監視テーブルを更新する(ステップ114)。ハードウェアに関するものでなければソフトウェア監視テーブルを更新する(ステップ116)。続いて、図5のメッセージテーブル19に対処方法が存在する場合には(ステップ118)、図5の障害解析モジュールを起動する(ステップ120)。対処方法が存在しない場合には、障害の原因のみを表示する(ステップ122)。対処方法が存在するかの判別は図6B<メッセージテーブル>の事例件数が0かどうかで行う。

【0019】続いて図5のハードウェア監視モジュール13の起動(ステップ130)から終了までの処理を説明する。ハードウェア監視モジュール13では、障害解析が終わるまで(ステップ132)、ハードウェア管理テーブル20にハードウェアの稼動状況を格納する(ステップ134)。

【0020】続いて図5のソフトウェア監視モジュール14の起動(ステップ140)から終了までの処理を説明する。ソフトウェア監視モジュール14では、障害解析が終わるまで(ステップ142)、ソフトウェア管理テーブル21にソフトウェアの稼動状況を格納する(ステップ144)。

【0021】続いて図5の障害解析モジュール15の起動(ステップ150)から終了までの処理を説明する。まず、過去の事例の中から最適事例を求める際に用いるカウンタを1にする(ステップ152)。まず、カウンタが図6B<メッセージテーブル>の事例件数より大き

いかを判別する(ステップ154)。大きくない場合、カウンタの示す順番に格納されている事例の履歴蓄積テーブルと作業履歴蓄積テーブルとのメッセージIDをキーとしたマッチング結果の図6C<対処テーブル>の履歴確信度へ格納する。続いて、カウンタの示す順番に格納されている事例の図6A<履歴蓄積テーブル>のソフトウェア/ハードウェア監視テーブルと図7D及びEのソフトウェア/ハードウェア監視テーブルとのハードウェア/ソフトウェア名及び監視項目をキーとしたマッチングの結果を監視確信度へ格納する。続いて、カウンタに1を加える(ステップ168)。カウンタが図6B<メッセージテーブル>の事例件数より大きい場合、以下の処理を行う(ステップ154)。履歴確信度が最大の事例を最適事例とし(履歴確信度が最大の事例が複数存在する際には、監視確信度が最大の事例とする)、障害の原因の表示と過去の最適事例表示を行う(ステップ156)。続いて、図6C<対処テーブル>の自動/手動対処設定を参照し、対処が自動設定になっているかを判別する(ステップ158)。自動設定になっていない場合、対処モジュールを起動し、人による対処を行う(ステップ166)。自動設定になっている場合、図6C<対処テーブル>の対処コマンド及び対処確認コマンドを実行する(ステップ160)。続いて、障害回復したどうかを図7F<対処履歴テーブル>の対処結果と対処確認結果を比較して判別し(ステップ162)、回復した場合には障害回復の表示を行う(ステップ164)。回復していない場合、対処モジュールを起動し、人による対処を行う(ステップ166)。

【0022】続いて図5の対処モジュール16の起動(ステップ170)から終了までの処理を説明する。まず、人による対処入力を待ち(ステップ172)、入力後、図7F<対処履歴テーブル>に対処結果及び対処確認結果を格納する(ステップ174)。障害回復したどうかを図7F<対処履歴テーブル>の対処結果と対処確認結果を比較して判別し(ステップ176)、回復した場合には障害回復の表示を行う(ステップ178)。回復していない場合、人による対処を行う(ステップ172、174、176)。

【0023】

【発明の効果】以上述べたように、本発明によれば、複数のハードウェア装置及びソフトウェアから構成されるオンラインシステムの障害にリアルタイムな対処を可能とすることができるので、障害発生による損害を最小限に抑えることが出来る。また、従来人間が行っていた複雑な障害回復作業を機械化して支援することにより、専門の知識を持たない人でも障害回復作業を行うことができる。

【図面の簡単な説明】

【図1】本発明の処理手順の実施の形態を示すフローチャートである。

【図2】本発明の処理手順の実施の形態を示すフローチャートである。

【図3】本発明の処理手順の実施の形態を示すフローチャートである。

【図4】本発明の処理手順の実施の形態を示すフローチャートである。

【図5】本発明に係わるオンラインシステム障害解析方法を構成するシステムブロック図である。

【図6】本発明に係わるオンラインシステム障害解析システムを構成するデータテーブルである。

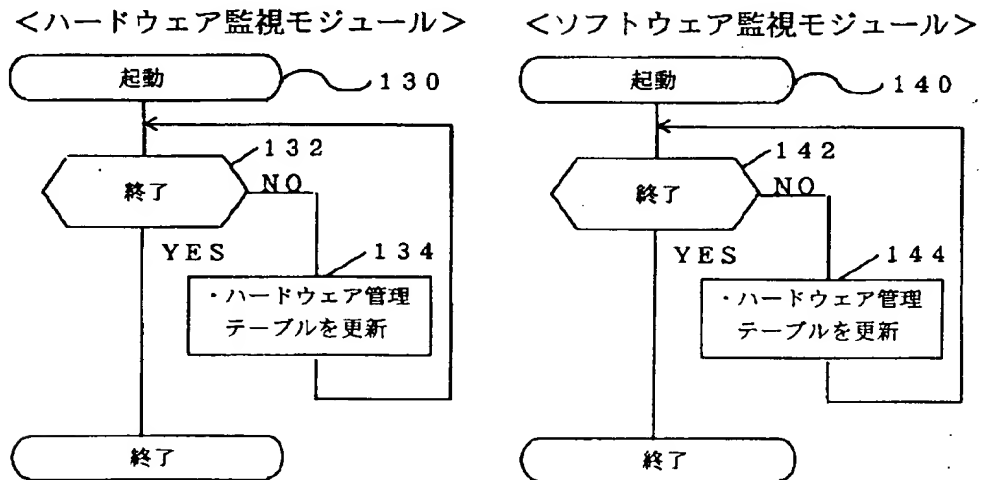
【図7】本発明に係わるオンラインシステム障害解析システムを構成するデータテーブルである。

【符号の説明】

- 10 オンラインシステム
- 11 メッセージ取得部
- 12 メッセージ監視モジュール
- 13 ハードウェア監視モジュール
- 14 ソフトウェア監視モジュール
- 15 障害解析監視モジュール
- 16 対処モジュール
- 17 履歴蓄積テーブル
- 18 作業履歴蓄積テーブル
- 19 メッセージテーブル
- 20 ハードウェア監視テーブル
- 21 ソフトウェア監視テーブル
- 22 対処履歴監視テーブル。

【図2】

図2



【図7】

図7

D <ハードウェア監視テーブル>

順番	ハードウェア名	監視項目	結果
1	H1	電圧	ON
2	H2	電圧	OFF
		電圧	ON
:	:	:	:

E <ソフトウェア監視テーブル>

順番	ソフトウェア名	監視項目	結果
1	S1	起動	ON
2	S2	起動	ON
:	:	:	:

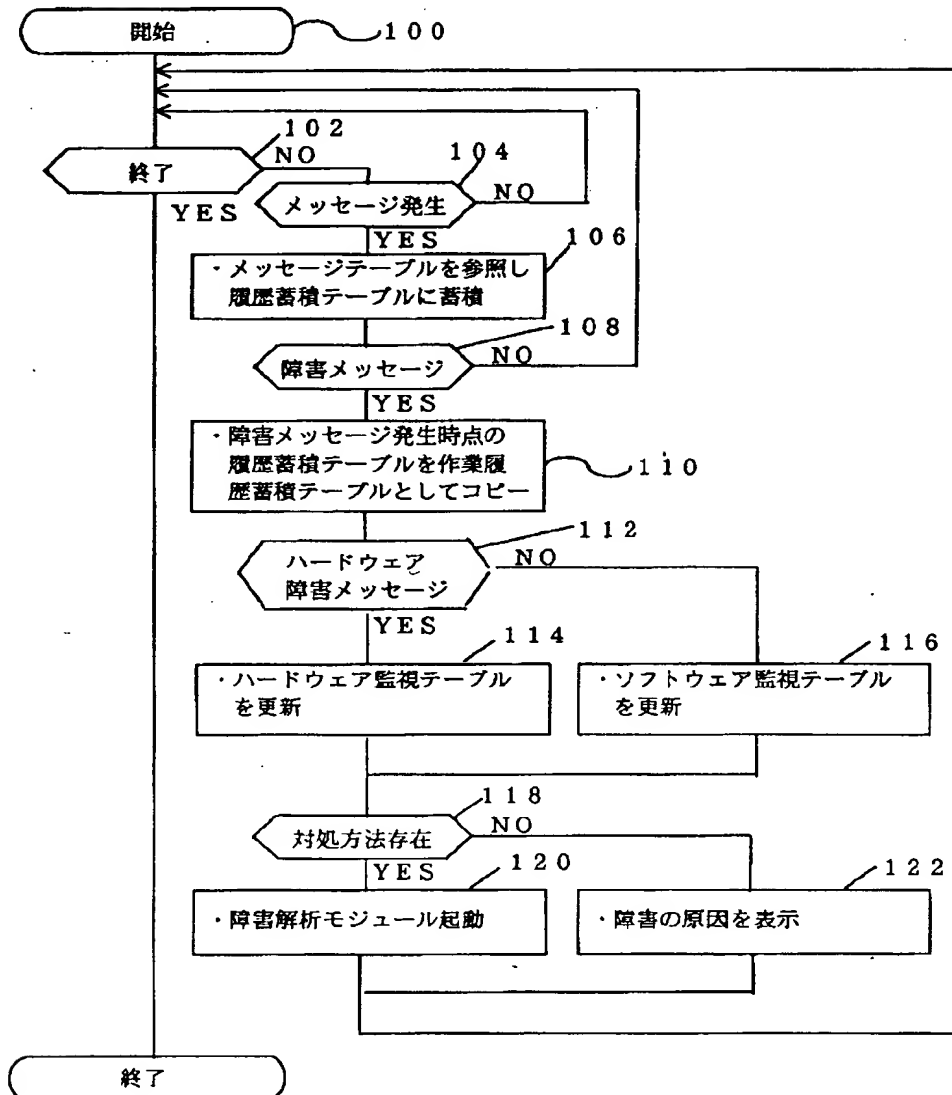
F <対処履歴テーブル>

メッセージID	対処テーブル
H5W002	
S4W001	
:	:

【図1】

図1

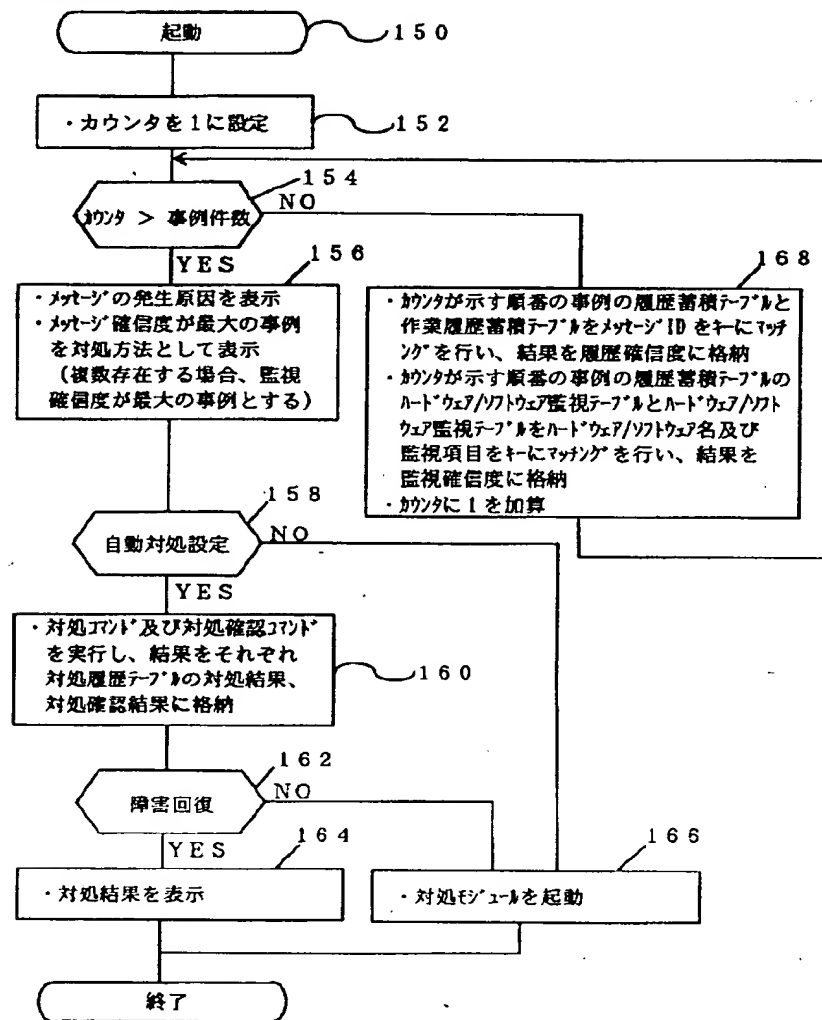
<メッセージ履歴管理モジュール>



【図3】

図3

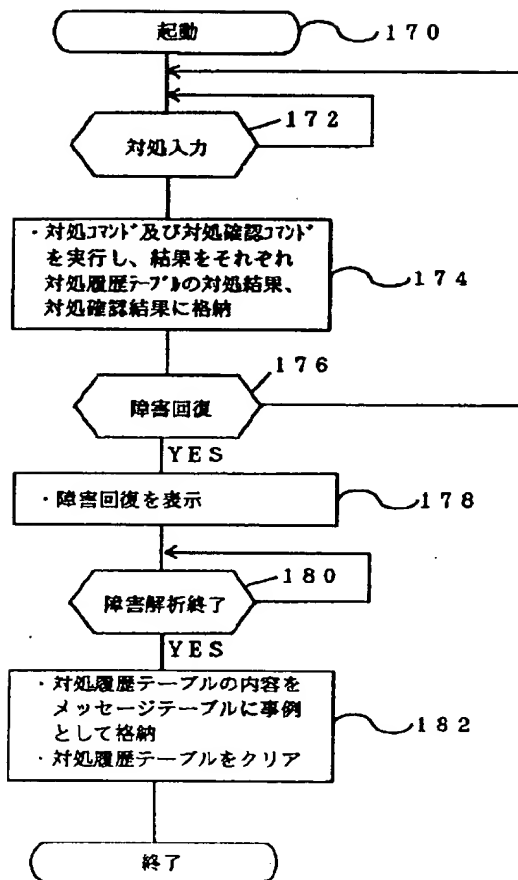
<障害解析モジュール>



【図4】

図4

<対処モジュール>



【図6】

図6

A <履歴蓄積テーブル、作業履歴蓄積テーブル>

項番	メッセージID	発生時刻	エリア/ハード 区分 #1	障害/警告 区分 #2	メッセージ
1	BSMO01	10:40:00	2	1	AAAAAAAAAA
2	BSMO02	10:40:10	2	1	BBBBBBBBBB
3	SAW001	10:40:15	1	1	PPPPPPPP
4	SSMO01	10:40:30	1	1	VVVVVVVV
5	SSMO01	10:40:40	2	2	WWWWWW
:	:	:	:	:	:

#1...エリア:1、ハード:2 #2...警告:1、障害:2

B <メッセージテーブル>

ハード /エリア 区分 #1	メッセージ 区分 #2	項番	メッセージ ID	障害/ 警告 区分 #3	原因	履歴 度	事例 件数	事例	
								履歴蓄積 テーブル1	対処 テーブル1
1	1	1	BSMO01	1	電圧	4	0		
		2	BSMO02	1	電圧	4	3		
	2	1	HAW001	1	アラーム不能	4	0		
		2	HAW001	2	アラーム不能	8	3		
		:	:	:	:	:	:		
		:	:	:	:	:	:		
2	1	1	SSMO01	1	起動不能	4	0		
		2	SSMO01	2	起動不能	12	2		
	2	1	SAW001	1	設定エラー	4	0		
		2	SAW001	2	設定エラー	8	2		
		:	:	:	:	:	:		
		:	:	:	:	:	:		

#1...ハードウェア:1、エリア:2 #2...メッセージ:1、アラーム/メッセージ:2 #3...警告:1、障害:2

C <対処テーブル>

対処履歴 テーブル	対処 結果	対処 結果	対処履歴 結果	履歴 確信度	履歴 確信度	自動/手動 設定 #1
AAA	BBB	CCC	DDD	CCC	4	3

#1...自動:1、手動:2

【図5】

図5

